CLAIMS

What is Claimed is:

1. A system for providing a firewall to a communication device, said system comprising:

a first device comprising a hardware implemented firewall, said first device coupled to a host device that is coupled to said communication device for establishing a connection to a network;

logic residing in said system to allow said communication device to establish a connection to the network provided said first device is in said system; and

said system configured to cause data transferred by the communication device to be processed by said firewall.

2. The system of Claim 1, further comprising:

logic for checking integrity of software components in said system.

3. The system of Claim 2, further comprising:

a server for providing policies to be used by said firewall; and

said first device further comprises stored values to access said server to receive the policies.

4. The system of Claim 1, further comprising:

a server for providing policies to be used by said firewall; and

said first device operable to access said server to receive the policies.

5. The system of Claim 4, wherein:

said system further comprises a plurality of nodes having a hardware implemented firewall; and wherein

said server is further operable to transfer the policies to said plurality of nodes, wherein said system comprises a centrally managed network having nodes with hardware implemented firewalls.

6. The system of Claim 1, wherein said logic to allow said system to establish a connection to the network comprises a hardware implemented token.

7. The system of Claim 1, further comprising a third device having stored thereon data needed to establish the connection to the network, said third device coupled to said first device, wherein said logic to allow said system to establish the connection is operable to access said data to assure said first device must be in said system to establish said connection to the network via the communication device.

8. The system of Claim 1, further comprising:
an alert log for logging possible breaches detected by said system.

9. The system of Claim 8, further comprising:
a configuration integrity checker for checking integrity of software components in said system, wherein said possible breach is detected by said configuration integrity checker.

10. The system of Claim 1, further comprising:
logic for preventing login of the host device unless said first device coupled to the host device.

11. The system of Claim 1, wherein said configuration integrity checker checks the integrity of software components residing in said host device.

12. The system of Claim 1, wherein said first device is physically coupled to the communication device, wherein the data transferred by the communication device to the network is processed by said firewall before it is transferred into the network and the data transferred from the network to the communication device passes through said firewall before it reaches the host device.

13. The system of Claim 12, wherein said physical connection is of the same medium as the network connection.

14. The system of Claim 12, wherein said physical connection comprises an MPCI (Mini Peripheral Component Interconnect) adapter to couple said first device to the communication device.

15. The system of Claim 1, wherein said system further comprises a software driver in the host device, said driver operable to pass data that is received by the communication device to said first device to be processed by said firewall.

16. The system of Claim 15, wherein said software driver is further operable to pass data which is to be transferred by the communication device over the network to said first device to be processed by said firewall.

17. The system of Claim 1, further comprising a software component installed above a driver for the communication device, said software component operable to route data for the communication device to said first device.

18. The system of Claim 17, wherein said software component is a shim that resides above a miniport driver.

19. The system of Claim 1, further comprising a software component installed below a driver for the communication device, said software component operable to route data for the communication device to said first device.

20. The system of Claim 1, further comprising:

transfer security logic residing on said first device, said transfer security logic for securely transferring data between said first device and a server in the network.

21. The system of Claim 1, further comprising:

a configuration integrity checker for checking integrity of software components in said system;

an alert log for logging possible security breaches detected by said system; and

a server for providing policies to be used by said firewall.

22. A method of providing security in a network having a communication interface device that makes a network connection without a firewall, said method comprising:

a) allowing a connection to said network to be established when using said communication interface device only if a firewall device comprising a hardware implemented firewall is coupled to a host device;

b) receiving data from said network over said connection establish via said communication interface device;

c) processing said data with said hardware implemented firewall; and

d) transferring said data to said host device, wherein said data is processed by said hardware implemented firewall.

23. The method of Claim 22, further comprising said host device routing said data to said firewall device to be processed by said hardware implemented firewall, said routing taking place at a physical layer in said data stack.

24. The method of Claim 22, further comprising:

e) sending policies to said firewall device, wherein the operation of said hardware implemented firewall is modified.

25. The method of Claim 22, further comprising:

e) performing a configuration integrity check of a software component on said host device.

26. The method of Claim 25, wherein said configuration integrity check is performed before said network connection is allowed in a), wherein said connection is allowed only if said configuration integrity check passes.

27. The method of Claim 25, wherein e) comprises performing said configuration integrity check by performing a hash on said software component to produce a hash value and comparing said hash value with a stored hash value.

28. The method of Claim 27, wherein said stored hash value resides on said firewall device.

29. The method of Claim 27, further comprising:

f) sending an alert if said configuration integrity check fails.

30. The method of Claim 29, further comprising:

g) storing an alert if said configuration integrity check fails.

31. The method of Claim 22, further comprising:

e) swapping resource spaces in said host device that are reserved for said communication interface device and said firewall device, wherein said host device treats said communication interface device as said firewall device and vice versa; and

f) said communication interface device transferring data received from said network in b) to said firewall device, wherein said firewall device processes said data with said hardware implemented firewall.

32. The method of Claim 22, further comprising:

e) transferring data to be transferred over said network by said communication interface device to said firewall device; and

f) processing said data with said hardware implemented firewall, wherein said data is processed by said hardware implemented firewall before it is transferred over said network connection established via said communication interface device.

33. The method of Claim 32, wherein said e) comprises said host device routing said data to said firewall device before it is sent to said communication interface device, said routing taking place at a physical layer in said data stack.

34. The method of Claim 22, further comprising:

e) performing a configuration integrity check of a software component on said host device; and

f) sending policies to said firewall device, wherein the operation of said hardware implemented firewall is modified.

35. The method of Claim 34, further comprising:

g) sending an alert if said configuration integrity check fails.

36. A firewall device for providing a hardware implemented firewall to a device for establishing a network connection, said device comprising:

a hardware implemented firewall;

a data interface for receiving and sending data;

first logic for allowing said network connection to be established using said device if said firewall device is coupled to said device.

37. The firewall device of Claim 36, further comprising:

logic for performing a configuration integrity check of software components, said logic operable to produce a numeric value that results from said check;

a stored value for each software component to be checked for integrity; and

logic to compare said produced value with said stored value.

38. The firewall device of Claim 36, wherein said first logic comprises stored values to be used in an authentication process during establishment of said network connection.